

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/000193

International filing date: 11 January 2005 (11.01.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-008507  
Filing date: 15 January 2004 (15.01.2004)

Date of receipt at the International Bureau: 03 March 2005 (03.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/JP2005/000193

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

13.01.2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 4 年   1 月 1 5 日  
Date of Application:

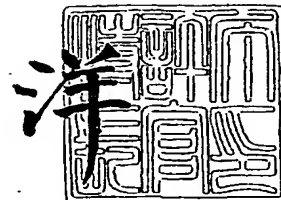
出 願 番 号            特 願 2 0 0 4 - 0 0 8 5 0 7  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 4 - 0 0 8 5 0 7 ]

出   願   人            松 下 電 器 産 業 株 式 会 社  
Applicant(s):

2 0 0 5 年   2 月 1 7 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



出証番号   出証特 2 0 0 5 - 3 0 1 1 4 6 2

【書類名】 特許願  
【整理番号】 2900750513  
【提出日】 平成16年 1月15日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04L 9/30  
【発明者】  
【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 パナソニックモバイルコミュニケーションズ株式会社内  
【氏名】 岩間 智大  
【発明者】  
【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 パナソニックモバイルコミュニケーションズ株式会社内  
【氏名】 金子 友晴  
【発明者】  
【住所又は居所】 神奈川県横浜市港北区綱島東四丁目3番1号 パナソニックモバイルコミュニケーションズ株式会社内  
【氏名】 石井 義一  
【特許出願人】  
【識別番号】 000005821  
【氏名又は名称】 松下電器産業株式会社  
【代理人】  
【識別番号】 100105050  
【弁理士】  
【氏名又は名称】 鷺田 公一  
【手数料の表示】  
【予納台帳番号】 041243  
【納付金額】 21,000円  
【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 9700376

## 【書類名】特許請求の範囲

## 【請求項 1】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システム。

## 【請求項 2】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線 LAN システムへの接続認証処理を行う認証処理部と、前記公衆無線 LAN システムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置の IP アドレスを取得するアドレス取得部と、前記移動無線端末装置の IP アドレスを前記接続認証サーバに通知するアドレス通知部と、前記仮想私設網中継装置の IP アドレスを用いて前記仮想私設網中継装置と IPsec 鍵交換を行う IPsec 鍵交換部と、を具備する移動無線端末装置。

## 【請求項 3】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線 LAN システムへの接続認証処理を行う認証処理部と、前記公衆無線 LAN システムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置との間で行う IPsec 鍵交換に用いる IPsec 事前共有秘密鍵を取得する IPsec 共有鍵取得部と、前記 IPsec 事前共有秘密鍵を用いて前記仮想私設網中継装置と IPsec 鍵交換を行う IPsec 鍵交換部と、を具備する移動無線端末装置。

## 【請求項 4】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線 LAN システムへの接続認証処理を行う認証処理部と、前記公衆無線 LAN システムへの接続が許可された時に前記接続認証サーバか

ら前記ホームエージェントとの間で行うモバイルIP登録に用いる事前共有秘密鍵を取得するMIP共有鍵取得部と、前記事前共有秘密鍵を用いて前記ホームエージェントへモバイルIP登録を行うMIP登録部と、を具備する移動無線端末装置。

【請求項5】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、

前記接続認証サーバに対して前記公衆無線LANシステムへの接続認証処理を行う認証処理部と、前記公衆無線LANシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のIPアドレスを取得するアドレス取得部と、前記移動無線端末装置のIPアドレスを前記接続認証サーバに通知するアドレス通知部と、前記接続認証サーバから前記仮想私設網中継装置との間で行うIPsec鍵交換に用いるIPsec事前共有秘密鍵を取得するIPsec共有鍵取得部と、前記接続認証サーバから前記ホームエージェントとの間で行うモバイルIP登録に用いるMIP事前共有秘密鍵を取得するMIP共有鍵取得部と、前記仮想私設網中継装置のIPアドレスと前記IPsec事前共有秘密鍵を用いて前記仮想私設網中継装置とIPsec鍵交換を行うIPsec鍵交換部と、前記MIP事前共有秘密鍵を用いて前記ホームエージェントへモバイルIP登録を行うMIP登録部と、を具備する移動無線端末装置。

【請求項6】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置のIPアドレスを受信するアドレス取得部と、前記移動無線端末装置のIPアドレスを用いて前記移動無線端末装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する仮想私設網中継装置。

【請求項7】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置との間で行うIPsec鍵交換に用いる事前共有秘密鍵を受信するIPsec共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する仮想私設網中継装置。

【請求項8】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、

前記接続認証サーバから前記移動無線端末装置のIPアドレスを受信するアドレス取得部と、前記接続認証サーバから前記移動無線端末装置との間で行うIPsec鍵交換に用いる事前共有秘密鍵を受信するIPsec共有鍵取得部と、前記移動無線端末装置のIPアドレスと前記事前共有秘密鍵を用いて前記移動無線端末装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する仮想私設網中継装置。

#### 【請求項9】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、

前記移動無線端末装置の前記公衆無線LANシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の前記公衆無線LANシステムへの接続を許可する時に前記移動無線端末装置のIPアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のIPアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のIPアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、を具備する接続認証サーバ。

#### 【請求項10】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、

前記移動無線端末装置の前記公衆無線LANシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線LANシステムへの接続を許可する時に前記移動無線端末装置と前記仮想私設網中継装置との間で行うIPsec鍵交換に用いる事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するIPsec共有鍵配布部と、を具備する接続認証サーバ。

#### 【請求項11】

公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LAN

アクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって

前記移動無線端末装置の前記公衆無線 LAN システムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線 LAN システムへの接続を許可する時に前記移動無線端末装置と前記ホームエージェントとの間で行うモバイル IP 登録に用いる事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布する MIP 共有鍵配布部と、を具備する接続認証サーバ。

【請求項 12】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって

前記移動無線端末装置の前記公衆無線 LAN システムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線 LAN システムへの接続を許可する時に前記移動無線端末装置の IP アドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置の IP アドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置の IP アドレスを前記仮想私設網中継装置に通知するアドレス通知部と、前記移動無線端末装置と前記仮想私設網中継装置との間で行う IPsec 鍵交換に用いる IPsec 事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布する IPsec 共有鍵配布部と、前記移動無線端末装置と前記ホームエージェントとの間で行うモバイル IP 登録に用いる MIP 事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布する MIP 共有鍵配布部と、を具備する接続認証サーバ。


【請求項 13】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける無線 LAN アクセスポイントであって、

前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順において確立した安全な通信路を用いて、前記接続認証サーバから送信される IP アドレスと IPsec 事前共有鍵、Mobile IP 事前共有鍵を前記移動無線端末装置に送信し、かつ、前記移動無線端末装置から送信される IP アドレスを前記接続認証サーバへ送信する認証中継部と、を具備する無線 LAN アクセスポイント。

【請求項 14】

公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN



アクセスポイントと、を具備する移動無線通信システムにおけるホームエージェントであって、

前記接続認証サーバから前記移動無線端末装置のモバイルIP登録に用いる事前共有秘密鍵を受信するMIP共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置からのモバイルIP登録を処理するMIP処理部と、を具備するホームエージェント。



## 【書類名】明細書

【発明の名称】移動無線通信システム、移動無線端末装置、仮想私設網中継装置及び接続認証サーバ

## 【技術分野】

## 【0001】

本発明は、公衆無線LANシステムなどの公衆網から私設網へアクセスするようなモバイルVPN接続環境において、セキュリティの高い通信路を確立するための移動無線通信システム、移動無線端末装置、仮想私設網中継装置及び接続認証サーバに関する。

## 【背景技術】

## 【0002】

公衆網から私設網への接続において、セキュアな通信路を確立するためにIPsec技術がIETFにより標準化されている。IPv6では、このIPsec技術をサポートすることが必須とされている。移動無線端末装置が公衆網と私設網を自由に移動可能なモバイル環境にIPsecを適用し、移動無線端末装置が公衆網から私設網へ接続することを想定する。この場合、移動無線端末装置は移動先の公衆網で使用可能なIPアドレスが移動の度にDHCP (Dynamic Host Configuration Protocol) などにより割り当てられる。即ち、移動無線端末装置の移動先によりIPアドレスが変化することになる。

## 【0003】

このため、私設網に設置されたIPsecトンネルの確立先であるセキュリティゲートウェイでは、各移動先でのIPアドレスが既知である必要があるため、移動無線端末装置のIPアドレスを用いたIPsec鍵交換を実施することが困難となるから、メインモードによるIPsecトンネルの確立が事実上不可能となる。従って、アグレッシブモードによるIPsecトンネルの確立が必要となるため、IPsecユーザID (ISAKMP IDペイロード) がネットワークを暗号化されない状態で流れることになるから、セキュリティの低下を招く。

## 【0004】

また、IPsecでは、IPsecトンネルを確立する双方において相互認証を行うための事前共有秘密鍵方式をサポートすることが必須となっている。しかし、一つの事前共有秘密鍵を使用し続けることによるセキュリティの低下が懸念される。そこで、事前共有秘密鍵を定期的に変更しセキュリティを保つことが考えられるが、ユーザ及び管理者の双方の負担が大きくなる。

## 【0005】

これまで、IPsecの認証に用いる事前共有秘密鍵を動的に配布するためのプロトコルとして、IETF (Internet Engineering Task Force) においてPIC (Pre-IKE Credential Provisioning Protocol) が提案されている (非特許文献1参照)。

## 【0006】

PICは、IPsecでも利用されているISAKMP (Internet Security Association and Key Management Protocol) を用いて移動無線端末装置と認証サーバとの間に安全な通信路を確立し、PICにおける認証に必要とされる認証情報を交換して認証を行う。この認証が成功すると、認証サーバはクレデンシャルと呼ばれるその後のIPsecの認証で利用する認証情報 (例えば、事前共有秘密鍵及び公開鍵証明書) を移動無線端末装置に発行する。

【非特許文献1】 “PIC, A Pre-IKE Credential Provisioning Protocol”、draft-ietf-ipsra-pic-06.txt、<http://www.ietf.org/internet-drafts/draft-ietf-ipsra-pic-06.txt>

## 【発明の開示】

## 【発明が解決しようとする課題】

## 【0007】

移動無線端末装置が公衆無線LANシステムなどの公衆網において、社内ネットワークなどの私設網に接続する場合に、移動無線端末装置はIPsecを用いて私設網とセキュアな

通信路、即ちIPsecトンネルを確立することが考えられる。

【0008】

しかし、この場合に、移動無線端末装置が公衆網と私設網を自由に移動可能なモバイル環境にIPsecを適用した場合には、移動無線端末装置のIPアドレスが移動の度に变化するため、IPsecメインモードによるIPsec鍵交換が困難である。このため、アグレッシブモードのIPsec鍵交換によるトンネルの確立が余儀なくされ、IPsecユーザIDがネットワークを暗号化されない状態で流れることとなりセキュリティの低下を招くことになるという問題がある。

【0009】

また、IPsecメインモードの鍵交換によるトンネルを確立するためには、移動無線端末装置の移動先でのIPアドレスが既知である必要がある。しかし、公衆無線LANシステムなどの公衆網においてはDHCPによりIPアドレスが割り当てられることが多いため、移動無線端末装置のIPアドレスを予め知ることは難しい。仮に移動無線端末装置の公衆無線LANシステムにおけるIPアドレスが既知である場合でも、公衆無線LANシステムにおける各IPアドレスに対してセキュリティポリシーを記述しておく必要があるため、セキュリティゲートウェイの性能が劣化し、また、管理者の管理の負担となるという問題がある。

【0010】

また、IPsecトンネルを確立する際の相互認証方式として、事前共有秘密鍵方式を適用した場合に、一つの事前共有鍵を使用し続けることは、時間と共にセキュリティが低下していくという問題がある。さらに、定期的に事前共有鍵を変更することが考えられるが、この場合には利用者と管理者の双方の負担となるという問題がある。

【0011】

前記問題を解決するために、IPsecの認証に用いる事前共有秘密鍵を動的に配布するプロトコルとしてPICが提案されている。しかし、PICを利用するためには、既存の装置にPICプロトコル機能を新たに追加する必要があるという問題がある。さらに、IPsecトンネル確立手順にPICを適用した場合に、PICによる移動無線端末装置と接続認証サーバとの間でISAKMP通信路の確立と、移動無線端末装置とセキュリティゲートウェイとの間でのISAKMP通信路の確立という移動無線端末装置にとって2度のISAKMPによる通信路を確立することになるため、手順が冗長であるから、IPsecトンネルの確立に要する時間が長くなるという問題がある。

【0012】

本発明は、かかる点に鑑みてなされたものであり、セキュリティの低下を防ぐことができ、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる移動無線通信システム、移動無線端末装置、仮想私設網中継装置及び接続認証サーバを提供することを目的とする。

【課題を解決するための手段】

【0013】

請求項1に記載の移動無線通信システムは、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する構成を採る。

【0014】

この構成によれば、移動無線端末装置は仮想私設網中継装置のIPアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得するこ

とができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのIPアドレスを用いてIPsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことができ、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPアドレスを送信することにより、IPアドレスを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0015】

請求項2に記載の移動無線端末装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線LANシステムへの接続認証処理を行う認証処理部と、前記公衆無線LANシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のIPアドレスを取得するアドレス取得部と、前記移動無線端末装置のIPアドレスを前記接続認証サーバに通知するアドレス通知部と、前記仮想私設網中継装置のIPアドレスを用いて前記仮想私設網中継装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する構成を採る。

#### 【0016】

この構成によれば、移動無線端末装置は仮想私設網中継装置のIPアドレスを取得することができる、かつ、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのIPアドレスを用いてIPsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことができ、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPアドレスを送信することにより、IPアドレスを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0017】

請求項3に記載の移動無線端末装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線LANシステムへの接続認証処理を行う認証処理部と、前記公衆無線LANシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置との間で行うIPsec鍵交換に用いるIPsec事前共有秘密鍵を取得するIPsec共有鍵取得部と、前記IPsec事前共有秘密鍵を用いて前記仮想私設網中継装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する構成を採る。

#### 【0018】

この構成によれば、移動無線端末装置と仮想私設網中継装置が同一のIPsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にIPsec事前共有秘密鍵を更新することができるため、セキュリティの低

下を防ぐことができ、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPsec事前共有秘密鍵を送信することにより、IPsec事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要があるため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0019】

請求項4に記載の移動無線端末装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線LANシステムへの接続認証処理を行う認証処理部と、前記公衆無線LANシステムへの接続が許可された時に前記接続認証サーバから前記ホームエージェントとの間で行うモバイルIP登録に用いる事前共有秘密鍵を取得するMIP共有鍵取得部と、前記事前共有秘密鍵を用いて前記ホームエージェントへモバイルIP登録を行うMIP登録部と、を具備する構成を採る。

#### 【0020】

この構成によれば、移動無線端末装置とホームエージェントが同一のMIP事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にMIP事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてMIP事前共有秘密鍵を送信することにより、MIP事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要があるため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0021】

請求項5に記載の移動無線端末装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける移動無線端末装置であって、前記接続認証サーバに対して前記公衆無線LANシステムへの接続認証処理を行う認証処理部と、前記公衆無線LANシステムへの接続が許可された時に前記接続認証サーバから前記仮想私設網中継装置のIPアドレスを取得するアドレス取得部と、前記移動無線端末装置のIPアドレスを前記接続認証サーバに通知するアドレス通知部と、前記接続認証サーバから前記仮想私設網中継装置との間で行うIPsec鍵交換に用いるIPsec事前共有秘密鍵を取得するIPsec共有鍵取得部と、前記接続認証サーバから前記ホームエージェントとの間で行うモバイルIP登録に用いるMIP事前共有秘密鍵を取得するMIP共有鍵取得部と、前記仮想私設網中継装置のIPアドレスと前記IPsec事前共有秘密鍵を用いて前記仮想私設網中継装置とIPsec鍵交換を行うIPsec鍵交換部と、前記MIP事前共有秘密鍵を用いて前記ホームエージェントへモバイルIP登録を行うMIP登録部と、を具備する構成を採る。

## 【0022】

この構成によれば、移動無線端末装置は仮想私設網中継装置のIPアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得することができるため、それぞれのIPアドレスを用いてIPsecメインモードによる鍵交換を開始することができ、かつ、移動無線端末装置と仮想私設網中継装置とは同一のIPsec事前共有秘密鍵を取得することが可能であるため移動無線端末装置の公衆無線LANシステムへの接続の度にIPsec事前共有秘密鍵を更新することができる。さらに、この構成によれば、移動無線端末装置とホームエージェントとは同一のMIP事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にMIP事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

## 【0023】

さらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPアドレスとIPsec事前共有秘密鍵とMIP事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

## 【0024】

請求項6に記載の仮想私設網中継装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置のIPアドレスを受信するアドレス取得部と、前記移動無線端末装置のIPアドレスを用いて前記移動無線端末装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する構成を採る。

## 【0025】

この構成によれば、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得することができるため、そのIPアドレスを用いてIPsecメインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

## 【0026】

請求項7に記載の仮想私設網中継装置は、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置との間で行うIPsec鍵交換に用いる事前共有秘密鍵を受信するIPsec共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置とIPsec鍵交換を行うIPsec鍵交換部と、を具備する構成を採る。

## 【0027】

この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のIPsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステム

ムへの接続の度に IPsec 事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイル VPN 接続環境における IPsec トンネルの確立に要する時間を短縮することができる。

#### 【0028】

請求項 8 に記載の仮想私設網中継装置は、公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける仮想私設網中継装置であって、前記接続認証サーバから前記移動無線端末装置の IP アドレスを受信するアドレス取得部と、前記接続認証サーバから前記移動無線端末装置との間で行う IPsec 鍵交換に用いる事前共有秘密鍵を受信する IPsec 共有鍵取得部と、前記移動無線端末装置の IP アドレスと前記事前共有秘密鍵を用いて前記移動無線端末装置と IPsec 鍵交換を行う IPsec 鍵交換部と、を具備する構成を採る。

#### 【0029】

この構成によれば、仮想私設網中継装置は移動無線端末装置の IP アドレスを取得することができるため、その IP アドレスを用いて IPsec メインモードによる鍵交換を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一の IPsec 事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線 LAN システムへの接続の度に IPsec 事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイル VPN 接続環境における IPsec トンネルの確立に要する時間を短縮することができる。

#### 【0030】

請求項 9 に記載の接続認証サーバは、公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線 LAN システムへの接続認証を行う認証処理部と、前記移動無線端末装置の前記公衆無線 LAN システムへの接続を許可する時に前記移動無線端末装置の IP アドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置の IP アドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置の IP アドレスを前記仮想私設網中継装置に通知するアドレス通知部と、を具備する構成を採る。

#### 【0031】

この構成によれば、移動無線端末装置は仮想私設網中継装置の IP アドレスを取得することができるため、かつ、仮想私設網中継装置は移動無線端末装置の IP アドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれの IP アドレスを用いて IPsec メインモードによる鍵交換を開始することができるから、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いて IP アドレスを送信することにより、IP アドレスを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイル VPN 接



続環境における IPsec トンネルの確立に要する時間を短縮することができる。

【0032】

請求項 10 に記載の接続認証サーバは、公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線 LAN システムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線 LAN システムへの接続を許可する時に前記移動無線端末装置と前記仮想私設網中継装置との間で行う IPsec 鍵交換に用いる事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布する IPsec 共有鍵配布部と、を具備する構成を採る。

【0033】

この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一の IPsec 事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線 LAN システムへの接続の度に IPsec 事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いて IPsec 事前共有秘密鍵を送信することにより、IPsec 事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイル VPN 接続環境における IPsec トンネルの確立に要する時間を短縮することができる。

【0034】

請求項 11 に記載の接続認証サーバは、公衆網と私設網と公衆無線 LAN システムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置と IPsec トンネルを確立し移動無線端末装置との間で IPsec トンネルを確立して前記移動無線端末装置の前記公衆無線 LAN システムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線 LAN システムに設置され前記移動無線端末装置の前記公衆無線 LAN システムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線 LAN の接続認証手順を中継する無線 LAN アクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線 LAN システムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線 LAN システムへの接続を許可する時に前記移動無線端末装置と前記ホームエージェントとの間で行うモバイル IP 登録に用いる事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布する MIP 共有鍵配布部と、を具備する構成を採る。

【0035】

この構成によれば、移動無線端末装置とホームエージェントとは同一の MIP 事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線 LAN システムへの接続の度に MIP 事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。また、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いて MIP 事前共有秘密鍵を送信することにより、MIP 事前共有秘密鍵を配布するためのセキュアな通信路を改めて確立する必要がないため、モバイル VPN 接続環境における IPsec トンネルの確立に要する時間を短縮することができる。

【0036】

請求項12に記載の接続認証サーバは、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける接続認証サーバであって、前記移動無線端末装置の前記公衆無線LANシステムへの接続認証を行う認証処理部と、前記移動無線端末装置の公衆無線LANシステムへの接続を許可する時に前記移動無線端末装置のIPアドレスを前記移動無線端末装置から受信するアドレス取得部と、前記仮想私設網中継装置のIPアドレスを前記移動無線端末装置に通知し、かつ、前記移動無線端末装置のIPアドレスを前記仮想私設網中継装置に通知するアドレス通知部と、前記移動無線端末装置と前記仮想私設網中継装置との間で行うIPsec鍵交換に用いるIPsec事前共有秘密鍵を前記移動無線端末装置と前記仮想私設網中継装置にそれぞれ配布するIPsec共有鍵配布部と、前記移動無線端末装置と前記ホームエージェントとの間で行うモバイルIP登録に用いるMIP事前共有秘密鍵を前記移動無線端末装置と前記ホームエージェントにそれぞれ配布するMIP共有鍵配布部と、を具備する構成を採る。

#### 【0037】

この構成によれば、移動無線端末装置は仮想私設網中継装置のIPアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのIPアドレスを用いてIPsecメインモードによるトンネル確立を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のIPsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にIPsec事前共有秘密鍵を更新することができる。さらに、この構成によれば、移動無線端末装置とホームエージェントが同一のMIP事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にMIP事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

#### 【0038】

またさらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPアドレスとIPsec事前共有秘密鍵とMIP事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0039】

請求項13に記載の無線LANアクセスポイントは、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおける無線LANアクセスポイントであって、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順において確立した安全な通信路を用いて、前記接続認証サーバから送信されるIPアドレスとIPsec事前共有鍵、Mobile IP事前共有鍵を前記移動無線端末装置に送信し、かつ、前記移動



無線端末装置から送信されるIPアドレスを前記接続認証サーバへ送信する認証中継部と、を具備する構成を採る。

#### 【0040】

この構成によれば、移動無線端末装置が仮想私設網中継装置のIPアドレスを取得することができ、かつ、仮想私設網中継装置は移動無線端末装置のIPアドレスを取得することができるため、移動無線端末装置と仮想私設網中継装置とはそれぞれのIPアドレスを用いてIPsecメインモードによる鍵交換を開始することができる。また、この構成によれば、移動無線端末装置と仮想私設網中継装置とは同一のIPsec事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にIPsec事前共有秘密鍵を更新することができる。これにより、セキュリティの低下を防ぐことが可能であり、かつ、ユーザ及び管理者の特別な作業を必要としない。

#### 【0041】

さらに、この構成によれば、移動無線端末装置と接続認証サーバにおいて接続認証手順により確立されたセキュアな通信路を用いてIPアドレスとIPsec事前共有秘密鍵とMIP事前共有秘密鍵を送信することにより、これらを配布するためのセキュアな通信路を改めて確立する必要がないため、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【0042】

請求項14に記載のホームエージェントは、公衆網と私設網と公衆無線LANシステムとを具備し、前記公衆網を介して前記私設網に設置された網中継装置とIPsecトンネルを確立し移動無線端末装置との間でIPsecトンネルを確立して前記移動無線端末装置の前記公衆無線LANシステムから前記私設網への接続を中継する仮想私設網中継装置と、前記移動無線端末装置の移動制御を行うホームエージェントと、前記公衆無線LANシステムに設置され前記移動無線端末装置の前記公衆無線LANシステムへの接続を認証する接続認証サーバと、前記移動無線端末装置と前記接続認証サーバとの間で行われる公衆無線LANの接続認証手順を中継する無線LANアクセスポイントと、を具備する移動無線通信システムにおけるホームエージェントであって、前記接続認証サーバから前記移動無線端末装置のモバイルIP登録に用いる事前共有秘密鍵を受信するMIP共有鍵取得部と、前記事前共有秘密鍵を用いて前記移動無線端末装置からのモバイルIP登録を処理するMIP処理部と、を具備する構成を採る。

#### 【0043】

この構成によれば、ホームエージェントはMIP事前共有秘密鍵を取得することが可能であり、かつ、移動無線端末装置の公衆無線LANシステムへの接続の度にMIP事前共有秘密鍵を更新することができるため、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【発明の効果】

#### 【0044】

以上説明したように、本発明によれば、セキュリティの低下を防ぐことが可能であり、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮することができる。

#### 【発明を実施するための最良の形態】

#### 【0045】

本発明の骨子は、移動無線端末装置が公衆無線LANシステムから公衆網を介して私設網に接続する時に移動無線端末装置と接続認証サーバとの間で行う接続認証手順において確立した暗号化通信路を用いて、移動無線端末装置と仮想私設網中継装置のIPアドレスを互いに通知する。

#### 【0046】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

#### (一実施の形態)

図1に示すように、本発明の一実施の形態に係る移動無線通信システム100は、公衆網101、私設網102、公衆無線LANシステム103、網中継装置104、仮想私設網中継装置105及びホームエージェント106を具備している。公衆無線LANシステム103は、公衆無線LAN107、接続認証サーバ108、無線LANアクセスポイント109及び複数の移動無線端末装置110（1つのみが図示されている）を具備している。

#### 【0047】

仮想私設網中継装置105は、私設網102に設置された網中継装置104と公衆網101を介してIPsecトンネルを静的に確立しており、仮想私設網中継装置105と私設網102との間のセキュアな通信を実現している。また、仮想私設網中継装置105は、公衆無線LANシステム103に存在する移動無線端末装置110との間でIPsecトンネルを確立し、移動無線端末装置110の公衆無線LANシステム103から私設網102への接続を中継する。なお、仮想私設網中継装置105と移動無線端末装置110とのIPsecトンネルは、移動無線端末装置110の公衆無線LANシステム103への接続の度に動的に確立し、また、移動無線端末装置110からの私設網102への接続要求の度に動的に確立する。

#### 【0048】

接続認証サーバ108は、移動無線端末装置110の公衆無線LAN107への接続認証を行う。この時に、無線LANアクセスポイント109は、移動無線端末装置110と接続認証サーバ108との間で行われる接続認証手順を中継する役割を果たす。

#### 【0049】

図2は、本発明の一実施の形態に係る移動無線端末装置110の構成を示すブロック図である。図3は、本発明の一実施の形態に係る仮想私設網中継装置105の構成を示すブロック図である。図4は、本発明の一実施の形態に係る接続認証サーバ108の構成を示すブロック図である。図5は、本発明の一実施の形態に係る無線LANアクセスポイント109の構成を示すブロック図である。図6は、本発明の一実施の形態に係るホームエージェント106の構成を示すブロック図である。

#### 【0050】

図2に示すように、移動無線端末装置110は、認証処理部201、アドレス通知部202、アドレス取得部203、IPsec共有鍵取得部204、IPsec鍵交換部205、MIP共有鍵取得部206及びMIP登録部207を具備している。なお、移動無線端末装置110は、移動無線通信を行う装置（図示せず）を具備している。

#### 【0051】

図3に示すように、仮想私設網中継装置105は、アドレス取得部301、IPsec共有鍵取得部302及びIPsec鍵交換部303を具備している。図4に示すように、接続認証サーバ108は、認証処理部401、アドレス通知部402、アドレス取得部403、IPsec共有鍵配布部404及びMIP共有鍵配布部405を具備している。図5に示すように、無線LANアクセスポイント109は、認証中継部501を具備している。図6に示すように、ホームエージェント106は、MIP共有鍵取得部601及びMIP処理部602を具備している。

#### 【0052】

次に、公衆無線LANシステム103に存在する移動無線端末装置110が私設網102に接続する場合の手順を例にとって説明する。

#### 【0053】

移動無線端末装置110が公衆無線LANシステム103の通信範囲内に存在する時に、移動無線端末装置110の認証処理部201は、公衆無線LANシステム103に接続するために、無線LANアクセスポイント109の認証中継部501を介して接続認証サーバ108の認証処理部401へ接続要求を送信する。公衆無線LANシステム103へ接続するためのプロトコルとして、IEEE（the Institute of Electrical and Electronics Engineers）で規定されている802.1xなどが挙げられる。

## 【0054】

以下、説明の簡単のため、802.1xを用いた場合の手順を説明する。802.1xの枠組みでは、移動無線端末装置110と無線LANアクセスポイント109の間では、EAP (Extensible Authentication Protocol) プロトコルが適用される。また、無線LANアクセスポイント109と接続認証サーバ108の間では、RADIUS (Remote Authentication Dial In User Service) プロトコルなどが適用される。無線LANアクセスポイント109は、前記両者のプロトコルを中継するブリッジ機能を有する。

## 【0055】

接続認証サーバ108の認証処理部401は、最初に、移動無線端末装置110の認証処理部201から送信されてくる接続要求の認証を行う。この認証は、EAP-MD5、EAP-TLS、EAP-LEAP又はPEAPといった種々の認証方式より行われる。ここでは説明の簡単のため、EAP-TLSを適用した場合の手順を説明する。EAP-TLSでは、移動無線端末装置110と接続認証サーバ108との間で電子証明書を交換することにより、相互の認証を行う。

## 【0056】

また、同時に、移動無線端末装置110と接続認証サーバ108は、乱数を交換して擬似乱数関数などによる演算処理を行うことにより、相互に共通のマスターシークレットを保持する。移動無線端末装置110と接続認証サーバ108は、前記マスターシークレットからPMK (Pairwise Master Key) を生成する。そして、接続認証サーバ108において移動無線端末装置110の認証が成功した場合、移動無線端末装置110と接続認証サーバ108は前記マスターシークレットを用いて、接続認証サーバ108と移動無線端末装置110との間の通信路を暗号化する。

## 【0057】

この時、無線LANアクセスポイント109の認証中継部501は前記通信路を中継する役割を果たすため、移動無線端末装置110と接続認証サーバ108の秘匿通信が可能となる。即ち、移動無線端末装置110の認証処理部201と無線LANアクセスポイント109の認証中継部501と接続認証サーバ108の認証処理部401との間でセキュアな通信路が確立されたことになる。以後、特別な断りがない限り、移動無線端末装置110と無線LANアクセスポイント109と接続認証サーバ108との通信は、このセキュアな通信路を用いて行う。

## 【0058】

そして、接続認証サーバ108は、この暗号化されたセキュアな通信路を用いて無線LANアクセスポイント109にPMKを送信する。これにより、移動無線端末装置110と無線LANアクセスポイント109は、共有するPMKからWEPキーを生成し、公衆無線LANシステム103における無線通信区間通信路をWEPキーにより暗号化する。(図7のステップST1)。

## 【0059】

次に、移動無線端末装置110と接続認証サーバ108との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置110と仮想私設網中継装置105のIPアドレスを交換する。接続認証サーバ108のアドレス通知部402は、無線LANアクセスポイント109の認証中継部501を中継して移動無線端末装置110のアドレス取得部203へ仮想私設網中継装置105のIPアドレスを送信する(図7のステップST2)。

## 【0060】

なお、接続認証サーバ108は仮想私設網中継装置105のIPアドレスを予め保持しておくことなどが考えられる。仮想私設網中継装置105のIPアドレスを受信した移動無線端末装置110のアドレス取得部203は、アドレス通知部202へ信号を送る。そして、その信号を受信したアドレス通知部202は、自身に割り当てられたIPアドレスを無線LANアクセスポイント109の認証中継部501を介して接続認証サーバ108のアドレス取得部403へ送信する(図7のステップST3)。

## 【0061】

また、接続認証サーバ108と移動無線端末装置110とがIPアドレスを送受信するために、EAPプロトコルとEAPOLプロトコルは拡張される。接続認証サーバ108の認証処理部401と無線LANアクセスポイント109の認証中継部501とがIPアドレスを送受信するために、EAPプロトコルのメッセージタイプにEAP-IPADDRが新たに定義される。そして、接続認証サーバ108の認証処理部401は、無線LANアクセスポイント109の認証中継部501へRADIUSプロトコルのvendor specificフィールドの属性値としてIPアドレスを送信する。

## 【0062】

一方、移動無線端末装置110の認証処理部201と無線LANアクセスポイント109の認証中継部501とがIPアドレスを送受信するために、図8に示すEAPOLプロトコルのパケットタイプにEAPOL-IPADDRが新たに定義され、属性値としてIPアドレスを通知するためのaddrフォーマット(図9)は追加される。このEAPOL-IPADDRメッセージの受信は、移動無線端末装置110にとっては仮想私設網中継装置105のIPアドレスの受信を示し、無線LANアクセスポイント109にとっては移動無線端末装置110のIPアドレスの受信をそれぞれ示す。

## 【0063】

そして、接続認証サーバ108のアドレス通知部402は、移動無線端末装置110のIPアドレスを仮想私設網中継装置105のアドレス取得部301へ送信する(図7のステップST4)。

## 【0064】

以上の手順により、移動無線端末装置110と仮想私設網中継装置105は相互のIPアドレスを取得することができる。そして、移動無線端末装置110のIPsec鍵交換部205と仮想私設網中継装置105のIPsec鍵交換部303は、取得したIPアドレスを用いて、IPsecメインモードによる鍵交換を開始することができる。

## 【0065】

さらに、接続認証サーバ108は、移動無線端末装置110と接続認証サーバ108との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置110と仮想私設網中継装置105との間で行われるIPsecトンネル確立時に用いるIPsec事前共有秘密鍵を、移動無線端末装置110と仮想私設網中継装置105とに配布する。接続認証サーバ108の認証中継部401は、無線LANアクセスポイント109の認証中継部501にIPsec事前共有秘密鍵を送信する。このIPsec事前共有秘密鍵を受信した無線LANアクセスポイント109の認証中継部501は、IPsec事前共有秘密鍵をそのまま移動無線端末装置110の認証処理部201へ送信する(図7のステップST4)。

## 【0066】

なお、接続認証サーバ108の認証処理部401から移動無線端末装置110の認証処理部201へIPsec事前共有秘密鍵を送信するために、EAPプロトコルとEAPOLプロトコルは拡張される。接続認証サーバ108の認証処理部401が無線LANアクセスポイント109の認証中継部501へIPsec事前共有秘密鍵を送信するために、EAPプロトコルのメッセージタイプにEAP-IPSECKEYを新たに定義する。そして、RADIUSプロトコルのvendor specificフィールドの属性値としてIPsec事前共有秘密鍵を送信する。一方、無線LANアクセスポイント109の認証中継部501から移動無線端末装置110の認証処理部201へIPsec事前共有秘密鍵を送信するためにEAPOLプロトコルの鍵配布メッセージを用いる。この時、key descriptionフォーマットのdescriptor typeをIPsecとして、keyフィールドを用いてIPsec事前共有秘密鍵を通知する。

## 【0067】

そして、接続認証サーバ108のIPsec共有鍵配布部404は、移動無線端末装置110に送信したIPsec事前共有秘密鍵と同一のIPsec事前共有秘密鍵を仮想私設網中継

装置105のIPsec共有鍵取得部302へ送信する。

【0068】

なお、接続認証サーバ108から仮想私設網中継装置105への通信路は、IPsecトンネルを静的に確立し、IPsec事前共有秘密鍵が盗聴されないセキュアな通信路を実現する。さらに、接続認証サーバ108で保持するIPsec事前共有秘密鍵は、接続認証サーバ108が動的に生成することも可能であるし、また、別の鍵生成サーバなどから受信することなどが可能である。

【0069】

以上の手順により、移動無線端末装置110と仮想私設網中継装置105とは同一のIPsec事前共有秘密鍵を共有する。移動無線端末装置110のIPsec鍵交換部205と仮想私設網中継装置105のIPsec鍵交換部303は、共有したIPsec事前共有秘密鍵を用いて、IPsecメインモードによる鍵交換を開始する。仮想私設網中継装置105のIPsec鍵交換部303は、移動無線端末装置110のIPsec鍵交換部205からの認証要求に記載のIPsec事前共有秘密鍵とIPアドレスとユーザIDが仮想私設網中継装置105で保持するIPsec事前共有秘密鍵とIPアドレスとユーザIDと一致する場合に、移動無線端末装置110の認証を許可してIPsecトンネルを確立する。

【0070】

また、接続認証サーバ108は、移動無線端末装置110と接続認証サーバ108との間で共有するマスターシークレットにより暗号化された通信路を用いて、移動無線端末装置110がホームエージェント106への登録に用いるMIP事前共有秘密鍵を移動無線端末装置110へ送信する。接続認証サーバ108の認証処理部401は、MIP事前共有秘密鍵を無線LANアクセスポイント109の認証中継部501に送信する。このMIP事前共有秘密鍵を受信した無線LANアクセスポイント109の認証中継部501は、MIP事前共有秘密鍵を移動無線端末装置110の認証処理部201へ送信する。

【0071】

なお、接続認証サーバ108の認証処理部401が移動無線端末装置110の認証処理部201へMIP事前共有秘密鍵を送信するために、EAPプロトコルとEAPOLプロトコルは拡張される。接続認証サーバ108の認証処理部401が無線LANアクセスポイント109の認証中継部501へMIP事前共有秘密鍵を送信するために、EAPプロトコルのメッセージタイプにEAP-MIPKEYは新たに定義される。そして、接続認証サーバ108の認証処理部401は、無線LANアクセスポイント109の認証中継部501へRADIUSプロトコルのvendor-specificフィールドの属性値としてMIP事前共有秘密鍵を送信する。

【0072】

一方、無線LANアクセスポイント109の認証中継部501が移動無線端末装置110の認証処理部201へMIP事前共有秘密鍵を送信するためにEAPOLプロトコルの鍵配布メッセージが用いられる。この時、key descriptionフォーマットのdescriptor typeをMIPとして、keyフィールドを用いてMIP事前共有秘密鍵が通知される。

【0073】

そして、接続認証サーバ108のMIP共有鍵配布部405は、移動無線端末装置110に送信したMIP事前共有秘密鍵と同一のMIP事前共有秘密鍵と移動無線端末装置110のIPアドレスをホームエージェント106のMIP共有鍵取得部601へ送信する(図7のステップST5)。

【0074】

なお、接続認証サーバ108からホームエージェント106への通信路は、IPsecトンネルを静的に確立し、MIP事前共有秘密鍵が盗聴されないセキュアな通信路を実現する。さらに、接続認証サーバ108で保持するMIP事前共有秘密鍵は、接続認証サーバ108が動的に生成することも可能であるし、また、別の鍵生成サーバなどから受信することなどが可能である。

【0075】

以上の手順により、移動無線端末装置 110 とホームエージェント 106 は、同一の MIP 事前共有秘密鍵を共有する。移動無線端末装置 110 の MIP 登録部 207 は、MIP 事前共有鍵を用いてホームエージェント 106 の MIP 処理部 602 に対してモバイル IP 登録 (Binding Update) を行う。ホームエージェント 106 の MIP 処理部 602 は、移動無線端末装置 110 の MIP 登録部 207 からのモバイル IP 登録メッセージの認証フィールドに記載の MIP 事前共有秘密鍵と SPI がホームエージェント 106 で保持する MIP 事前共有秘密鍵と SPI と一致する場合に、移動無線端末装置 110 のモバイル IP 登録の認証を許可する。なお、既に移動無線端末装置 110 と仮想私設網中継装置 105 との間には IPsec トンネルが確立されているため、移動無線端末装置 110 とホームエージェント 106 との通信路はセキュアである。

#### 【0076】

このように、本発明の一実施の形態によれば、移動無線端末装置 110 が公衆無線 LAN システム 103 などの公衆網から私設網へ接続するようなモバイル VPN 接続環境において、IPsec メインモードによる IPsec トンネルを確立することが可能となる。また、本発明の一実施の形態によれば、移動無線端末装置 110 の公衆無線 LAN システム 103 へのアクセスの度に IPsec 事前共有鍵と MIP 事前共有鍵を動的に更新することができる。したがって、本発明の一実施の形態によれば、セキュリティの低下を防ぐことができ、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイル VPN 接続環境における IPsec トンネルの確立に要する時間を短縮することができる。

#### 【産業上の利用可能性】

#### 【0077】

本発明は、移動無線端末装置が公衆無線 LAN システムから公衆網を介して私設網へアクセスするモバイル VPN 環境を提供する移動無線通信システムとして好適である。

#### 【図面の簡単な説明】

#### 【0078】

【図 1】 本発明の一実施の形態に係る移動無線通信システムの構成を示す図

【図 2】 本発明の一実施の形態に係る移動無線端末装置の構成を示すブロック図

【図 3】 本発明の一実施の形態に係る仮想私設網中継装置の構成を示すブロック図

【図 4】 本発明の一実施の形態に係る接続認証サーバの構成を示すブロック図

【図 5】 本発明の一実施の形態に係る無線アクセスポイントの構成を示すブロック図

【図 6】 本発明の一実施の形態に係るホームエージェントの構成を示すブロック図

【図 7】 本発明の一実施の形態に係る移動無線通信システムを説明するためのシーケンス図

【図 8】 本発明の一実施の形態に係る移動無線通信システムに用いられる EAPOL メッセージフォーマットを説明するための図

【図 9】 本発明の一実施の形態に係る移動無線通信システムに用いられる addr メッセージフォーマットを説明するための図

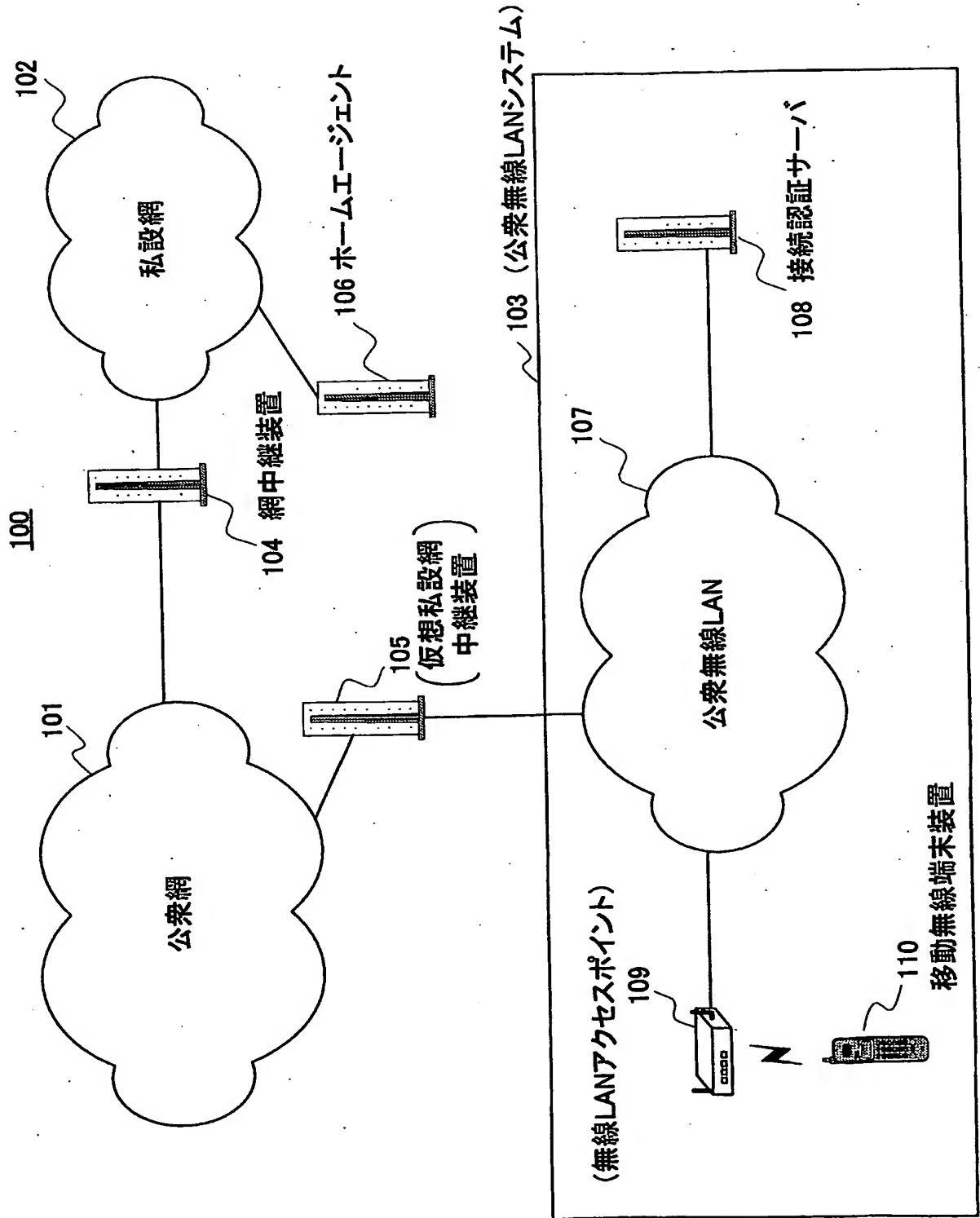
#### 【符号の説明】

#### 【0079】

- 100 移動無線通信システム
- 101 公衆網
- 102 私設網
- 103 公衆無線 LAN システム
- 104 網中継装置
- 105 仮想私設網中継装置
- 106 ホームエージェント
- 107 公衆無線 LAN
- 108 接続認証サーバ
- 109 無線 LAN アクセスポイント
- 110 移動無線端末装置

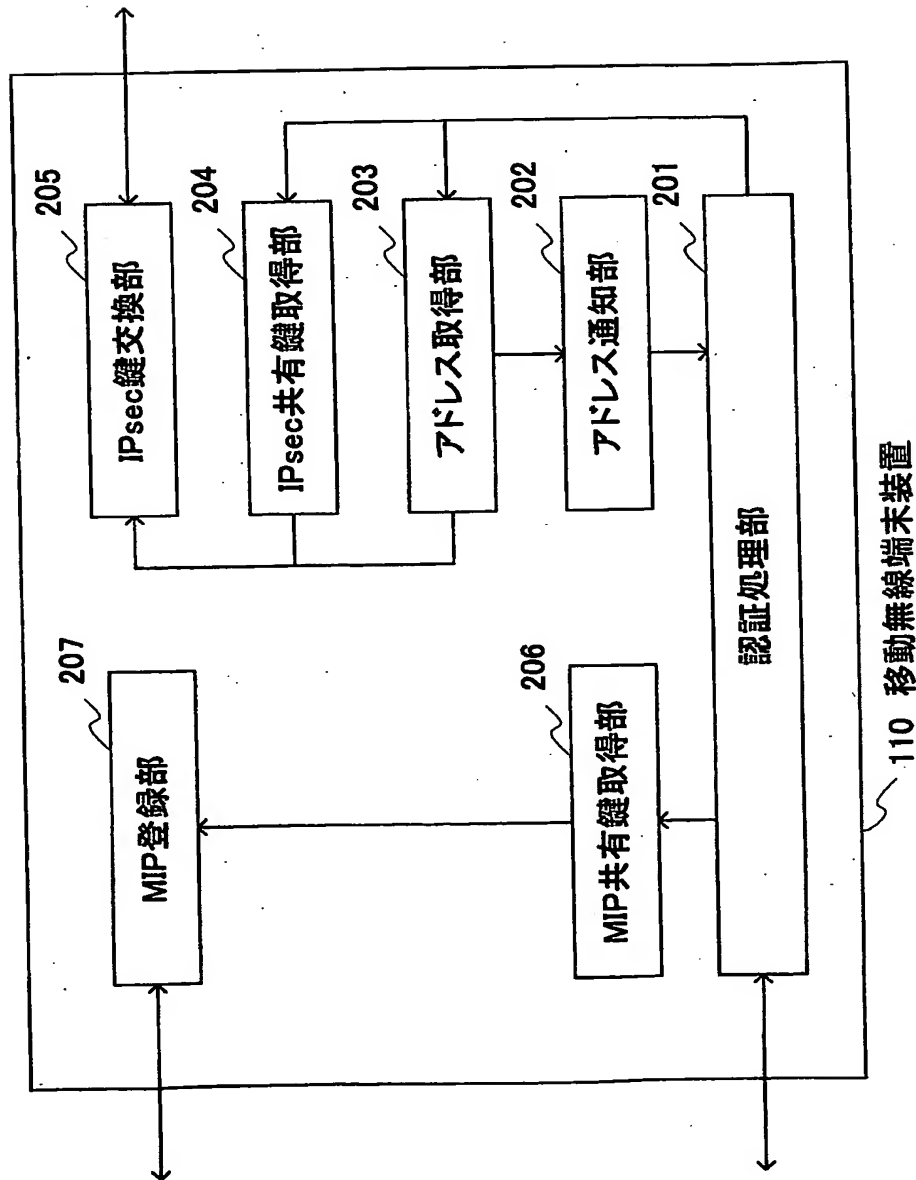
201 認証処理部  
202 アドレス通知部  
203 アドレス取得部  
204 IPsec共有鍵取得部  
205 IPsec鍵交換部  
206 MIP共有鍵取得部  
207 MIP登録部  
301 アドレス取得部  
302 IPsec共有鍵取得部  
303 IPsec鍵交換部  
401 認証処理部  
402 アドレス通知部  
403 アドレス取得部  
404 IPsec共有鍵配布部  
405 MIP共有鍵配布部  
501 認証中継部  
601 MIP共有鍵取得部  
602 MIP処理部

【書類名】 図面  
【図 1】

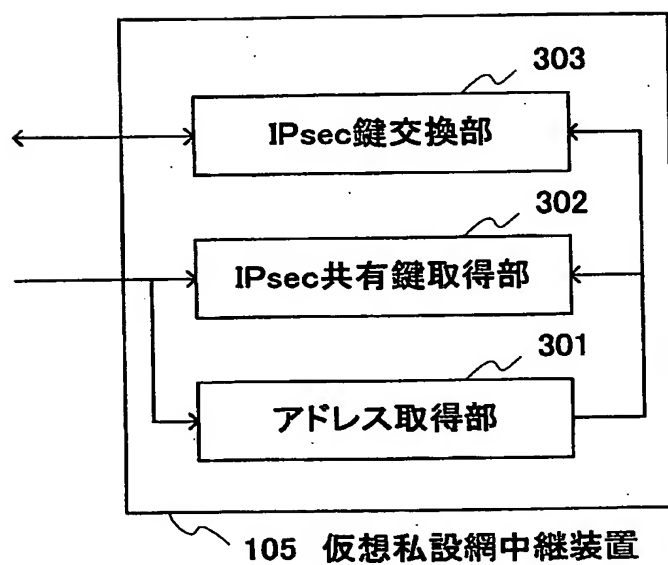




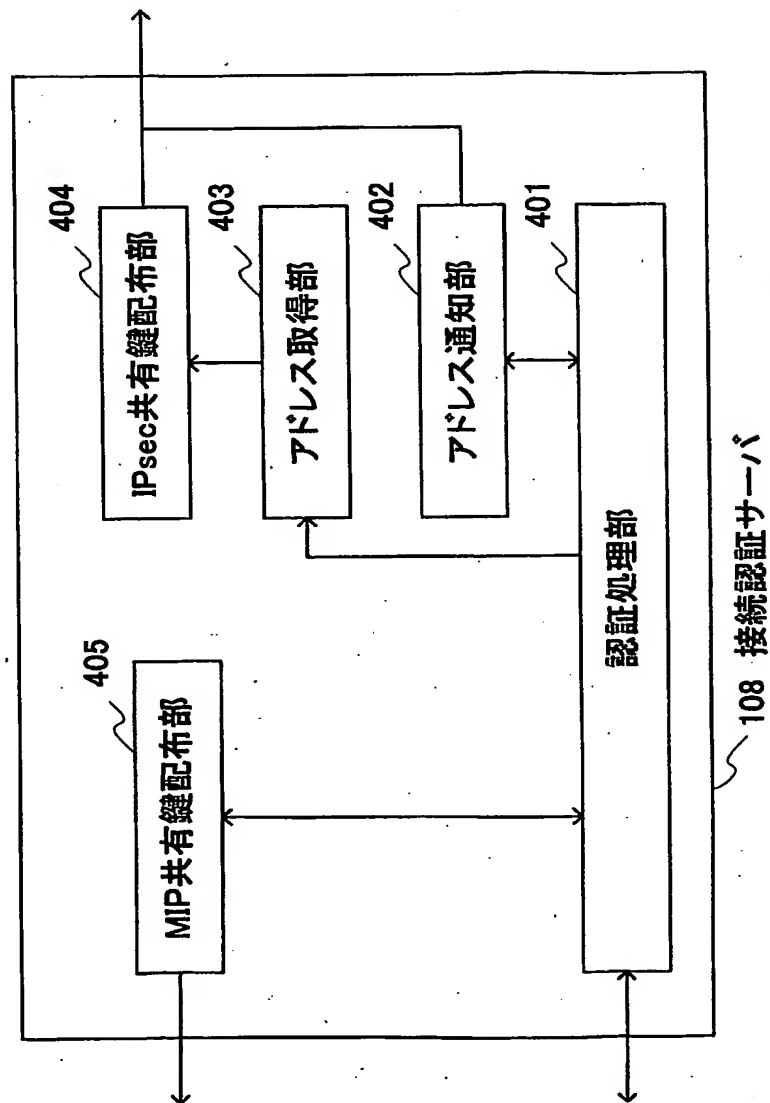
【図 2】



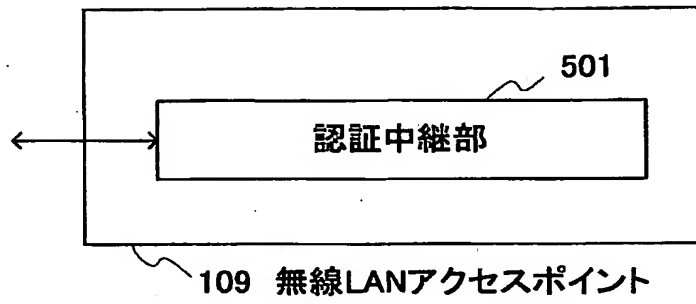
【図 3】



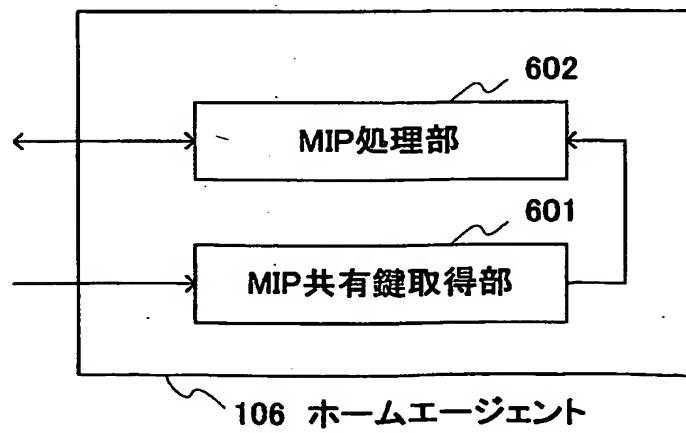
【図 4】



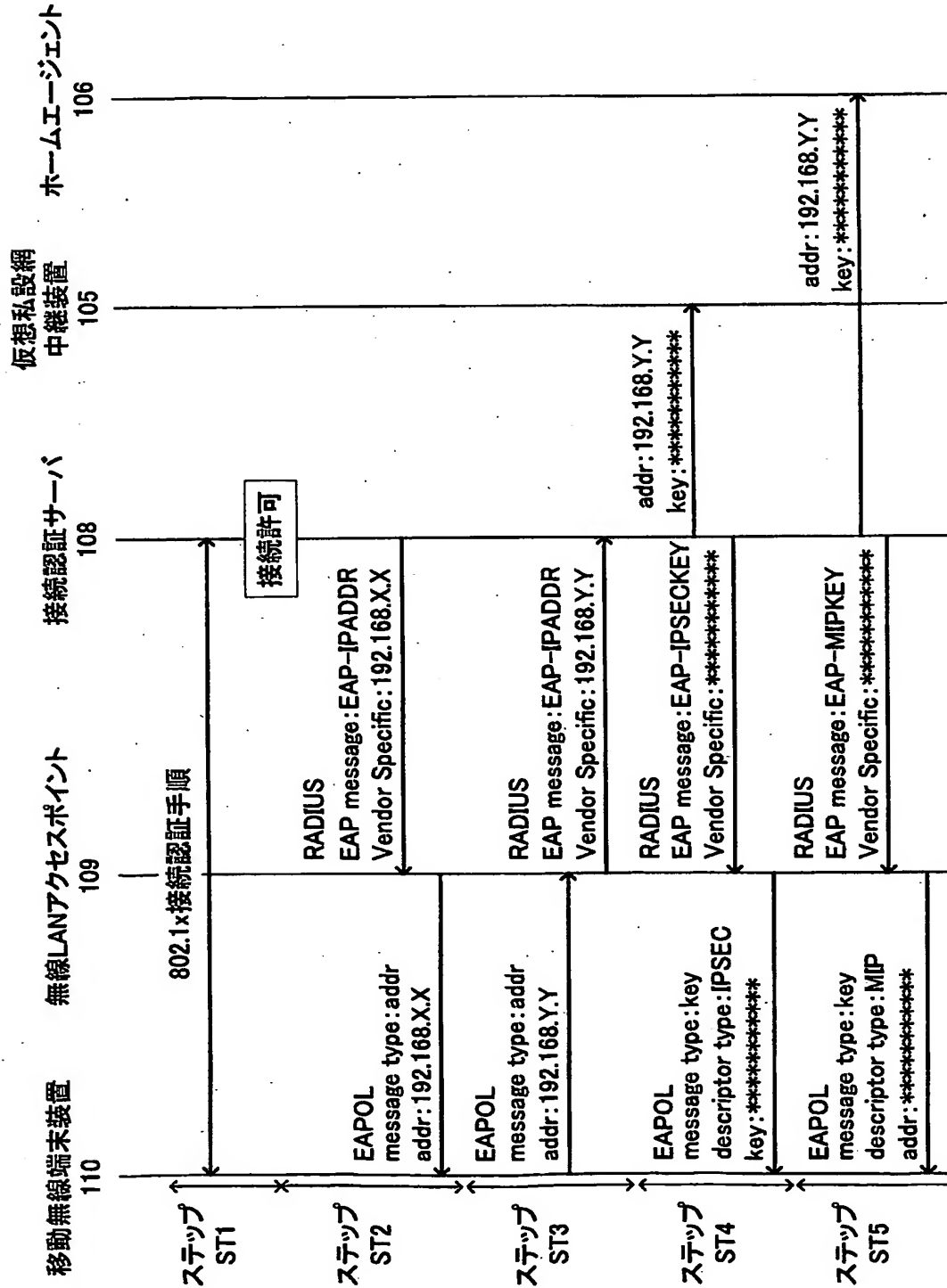
【図5】



【図6】



【図 7】



【図 8】

PAE Ethernet Type
Protocol Version
Packet Type
Packet Body Length
Packet Body

EAPOLメッセージフォーマット

【図 9】

Description Type
Length
IP Address

addrメッセージフォーマット

**【書類名】要約書****【要約】**

**【課題】** セキュリティの低下を防ぐことができ、ユーザ及び管理者の特別な作業を必要とせず、かつ、モバイルVPN接続環境におけるIPsecトンネルの確立に要する時間を短縮すること。

**【解決手段】** 本発明の移動無線通信システム100は、公衆網101を介して私設網102に設置された網中継装置104とIPsecトンネルを確立し移動無線端末装置110との間でIPsecトンネルを確立して移動無線端末装置110の公衆無線LANシステム103から私設網102への接続を中継する仮想私設網中継装置105と、移動無線端末装置110の公衆無線LANシステム103への接続を認証する接続認証サーバ108と、移動無線端末装置110と接続認証サーバ108との間で行われる公衆無線LAN107の接続認証手順を中継する無線LANアクセスポイント109と、を具備する。

**【選択図】** 図1

特願 2004-008507

出願人履歴情報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住所

大阪府門真市大字門真1006番地

氏名

松下電器産業株式会社